Identity Theft
Art Jones
Associate, Organized Change

According to the FTC, there were a total of 130 data breaches reported in the US in 2005. Those breaches exposed the personal information – such as Social Security and credit card numbers – of some 55 million Americans.

Workplace records are susceptible to theft. The federal government performed a study in 2003; result - Business Record theft that involves personal employee information = 90% of the total*. Federal Trade Commission report 2003*.

In May, a box of unencrypted tapes with information on 3.9 million Citi Financial customers, being shipped via UPS, never reached its intended destination. *Information Week March 13, 2006*

Fidelity Investments said that an employee laptop that was stolen during an offsite business meeting, contained the personal information – names, addresses, social security numbers, and more – on as many as 196,000 Hewlett Packard employees' who have Fidelity retirement accounts.

The list of victims of lost laptops stretches from the University of California Berkeley to the Justice Department to Bank of America and MCI. It's beginning to feel like if you haven't been stung by a report of a stolen company laptop yet, your number just hasn't come up. *Information Week March 27, 2006*

The prestigious Enterprise Strategy Group (ESG) produced a study in March 2006 that examines the policies, procedures, and technologies used by large organizations to safeguard, regulate, private, and company-confidential data. The results themselves are enough to make the most seasoned security analyst shudder.

For the purposes of the ESG study, confidential data was defined as information that can be categorized as:

- Intellectual property.
- Information that is protected by government regulation.
- Non-public private information (NPPI).
- Information that is protected by industry regulations.
- Information classified as company confidential or private.

The study found that distributed devices posed the biggest risk, with laptop computers being the most at risk.

Devices Used at Large Organizations* in North America that Pose the Biggest Security Risks according to information Security Professionals, 2006 (% of respondents)

- Laptop computers **68%**
- Desktop PCs **49%**
- Hard Copy **40%**
- Other mobile devices **40%**

Note: * defined as 1,000 – 20,000+ employees
Source: Enterprise Strategy Group, March 2006

ESG concludes:

- Confidential information is distributed throughout the enterprise.
- Control of confidential information decreases as a function of its location.
- **Insiders present the greatest threat for real data breach.**
- Responsibilities for protecting confidential data are extremely fragmented.
- Confidential data security policies are commonplace but enforcement lags behind.
- For the most part, technical defenses remain anchored to the network perimeter.

The image to the left shows well organized employee files, however the files are clearly exposed, and providing access to anyone within arm's length. Is the gentleman reaching high to retrieve a file folder that he is authorized to work upon? Is the gentleman a satisfied and loyal employee, using the information to complete a task on behalf of an employee/employer?

So what preventative measures can we put in place today to provide the best protection?

What to do:
Here are several tips that position you to provide protections for your company information stores.

Conduct a security audit.
Establish a baseline understanding for where you are.

Set realistic security objectives.
Define what you want to accomplish.

Create Policies.
Formulate a security policy.
Document a retention policy.
Develop a data backup policy.
Develop a proprietary information protection policy.
Develop sound personnel policies.
Develop security awareness training.

Implement Controls
Change management
Data classifications
Document classifications
Identity management

Implementing security is not an option anymore. Recent laws such as Sarbanes-Oxley, and other government mandated internal controls, are raising the bar. Implementing an information security program will not only reduce your vulnerability and risk, but also help you comply with the alphabet soup of new corporate governance, best practices, and government mandated regulations. In the end a good security methodology will help you protect your corporate information, while positioning you in the eyes of your business partners, customers, and business prospects, as a well organized forward thinking organization. And that can help your company generate more revenue.